Nombre : Emerson de la Cruz

Paralelo : B

Materia : Tic

1. Ciberataques
2. ¿Qué es un ciberataque? Un ciberataque es cualquier esfuerzo intencional para robar, exponer, alterar, deshabilitar o destruir datos, aplicaciones u otros activos a través del acceso no autorizado a una red, sistema informático o dispositivo digital.
3. Los ataques comienzan silenciosamente al hacer clic un enlace de un correo electrónico y al principio parece que no pasa nada pero es clic habré las puertas a los intrusos ‘Ciberataques’ y cuando llega el momento atacan, creando causa y confusión así

\*ILoveYOU fue un famoso ataque de malware lanzado en mayo del año 2000. Este ataque se considera uno de los más destructivos en la historia de la informática debido a su rápida propagación y al daño que causó a nivel mundial.

¿Qué era ILoveYOU?

ILoveYOU era un gusano informático que se propagaba principalmente a través de correos electrónicos. El correo electrónico tenía el asunto "ILOVEYOU" y un archivo adjunto llamado "LOVE-LETTER-FOR-YOU.txt.vbs". Al abrir el archivo adjunto, el script Visual Basic (VBS) se ejecutaba y realizaba varias acciones maliciosas:

Propagación: El gusano se enviaba automáticamente a todos los contactos de la libreta de direcciones de Microsoft Outlook del usuario infectado, lo que facilitó su rápida dispersión.

Modificación de archivos: Reemplazaba varios tipos de archivos, incluyendo imágenes y documentos, con copias del propio script del gusano. Esto resultaba en la pérdida de los archivos originales.

Recopilación de contraseñas: Intentaba robar contraseñas de acceso a internet almacenadas en el sistema y las enviaba a un servidor remoto.

El impacto de ILoveYOU fue masivo:

Extensión global: Afectó a decenas de millones de usuarios en todo el mundo en pocas horas.

Daños económicos: Se estima que los daños económicos causados por el gusano alcanzaron los 10 mil millones de dólares debido a la pérdida de datos y la interrupción de servicios.

Interrupciones: Grandes empresas, agencias gubernamentales y organizaciones alrededor del mundo tuvieron que desconectar sus sistemas de correo electrónico para detener la propagación del gusano

Respuesta y lecciones

La respuesta al ataque incluyó:

Desconexión de sistemas: Muchas organizaciones desconectaron sus servidores de correo electrónico para contener la propagación.

Actualización de seguridad: Las empresas y los usuarios comenzaron a tomar más en serio la importancia de mantener sus sistemas actualizados y protegidos con software antivirus.

El ataque de ILoveYOU resaltó la necesidad de mejorar las prácticas de seguridad cibernética, incluyendo la formación en seguridad para los empleados, la implementación de políticas de seguridad más estrictas, y el uso de tecnologías para detectar y prevenir la propagación de malware.

Documentales de: history y YouTube

## ¿Qué pasó con ILOVEYOU, el virus que infectó más de 50 millones de ordenadores y provocó un caos informático mundial?

En mayo del año 2000 el mundo vivía una revolución informática. Los ordenadores habían invadido todos los aspectos de la vida cotidiana, desde las oficinas gubernamentales hasta los hogares.

En su mayoría, con el sistema operativo Microsoft Windows. Internet empezaba a despegar y en un país como Estados Unidos, más del 43% de la población ya tenía acceso a la Red.

Ese aumento de la conectividad significaba que cada vez más personas dependían de los servicios en línea, incluido el correo electrónico.

### La propagación del virus

En ese momento miles de internautas recibieron en su bandeja de entrada un correo electrónico con las palabras “ILOVEYOU” (“Te quiero” en inglés) como asunto. El cuerpo del mensaje les invitaba a abrir una “carta de amor” como archivo adjunto y muchas personas así lo hicieron.

Sin embargo, no se trataba de un simple archivo de texto. En realidad, era un archivo VBScript con una extensión .VBS, aunque dicha extensión no era visible debido al diseño de la interfaz de usuario de Windows.

El archivo era en realidad un software malicioso (malware) que se propagaba a todos los contactos de Outlook de la víctima, hacía inaccesibles los archivos y robaba las contraseñas.

Veinte años después, ILOVEYOU [sigue recordándose](https://edition.cnn.com/2020/05/01/tech/iloveyou-virus-computer-security-intl-hnk/index.html) como uno de los virus de mayor alcance de la historia. Decenas de millones de ordenadores de todo el mundo se vieron afectados, la lucha por contener el malware y localizar a su autor fue protagonista de portadas en la prensa internacional, y sirvió como llamada de atención para el público sobre los peligros que plantean los cibercriminales.

### **Impacto: pérdidas económicas millonarias y daños colaterales**

Un[análisis](https://kb.iu.edu/d/aioe) de la Universidad de Indiana, en Estados Unidos, describe en detalle cómo funcionaba esta formidable trampa: cuando el usuario abría el archivo adjunto, éste se copiaba en el directorio de Windows y añadía sus propias claves al Registro para ejecutarse automáticamente cada vez que se iniciaba el ordenador.

A continuación, se dirigía a Internet Explorer: el malware sustituía la página de inicio del navegador por un enlace para descargar un ejecutable llamado [“WIN-BUGSFIX.exe”](https://www.bleepingcomputer.com/startups/6272/WIN_BUGSFIX.EXE/), que capturaba las contraseñas almacenadas en caché y las enviaba a una dirección de correo electrónico.

Además, escribía archivos para hacerlos inaccesibles y se propagaba a través de los canales disponibles de mIRC y los contactos de Microsoft Outlook. ILOVEYOU explotaba las macros instrucciones utilizadas habitualmente para automatizar tareas, pero también aprovechada en ocasiones por actores maliciosos.

También sacó a la luz vulnerabilidades con las que los expertos siguen lidiando hoy en día, a pesar de dos décadas de avances en seguridad y tecnología informática. Sólo que en aquella época, la concienciación sobre la [seguridad informática](https://www.pandasecurity.com/es/mediacenter/evolucion-antivirus-52-anos/) era aún limitada.

### **2,5 millones de ordenadores infectados**

En sólo una semana, más de 2,5 millones de ordenadores fueron infectados, y se estima que más del 10% de los equipos conectados a Internet en todo el mundo se vieron finalmente afectados por el ciberataque.

Alcanzó no sólo a ordenadores personales, sino también a corporaciones multinacionales y prestigiosas agencias gubernamentales como AT&T, Microsoft, Time Warner, Ford, el Pentágono, la CIA, la NASA y el Parlamento británico.

### **El autor, un joven filipino sin antecedentes penales**

Después de una amplia investigación, Onel de Guzmán, un joven de 27 años que trabajaba en un taller de reparación de teléfonos móviles en Manila (Filipinas), fue identificado como sospechoso. De Guzmán admitió ser el creador del gusano, [explicando que había diseñado el programa](https://www.bbc.com/news/technology-52458765) para obtener información de acceso a Internet de forma gratuita, ya que en aquel momento no podía permitirse pagarla.

Sin embargo, nunca llegó a ser condenado ni encarcelado por sus actividades, en gran medida porque aún no se habían creado leyes sobre delitos informáticos en aquel momento. Y hoy regenta un taller de reparación de smartphones en Manila.

Sitio web: https://www.google.com/amp/s/www.pandasecurity.com/es/mediacenter/iloveyou-virus/%3famp=1

.